

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1816	((713/170) or (705/51)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/16 16:46
S2	213	S1 and (@pd > "20060104")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 21:24
S3	6	(skeleton nest\$4 chain\$3) adj key with (encrypt\$3 encipher\$3 scrambl\$3 encod\$3) adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/17 19:11
S4	369	((726/28) or (726/29)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/12 15:36
S5	0	("2002/0023231").URPN.	USPAT	OR	ON	2006/06/17 19:51
S6	0	("7043760").URPN.	USPAT	OR	ON	2006/06/17 20:13
S7	14	("20010011351"   "20010020228"   "20010034708"   "20030034393"   "20030062411"   "20030173404"   "20040181675"   "6029195"   "6061789"   "6081793"   "6324648"   "6678516"   "6889325"   "6892944"). PN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/06/17 20:13
S8	503	((726/28) or (726/29)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/17 16:07
S9	36	S8 and (@pd > "20061120")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/12 15:37
S10	7	("20030115452"   "6085249"   "6199113"   "6304907"   "6487667"   "6690794"   "6721886").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/02/12 15:39
S11	2090	((713/170) or (705/51)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/16 16:47
S12	235	key adj encrypting adj key key adj upon adj key adj encryption	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/17 15:25

## EAST Search History

S13	7	skeleton adj key and encryption	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 20:18
S14	14	"6069957"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 20:18
S15	1	("6069957").PN.	US-PGPUB; USPAT	OR	OFF	2007/02/16 21:50
S16	3	key same rights adj management adj file	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 22:02
S17	1188	key same right adj management	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 22:02
S18	154	key same right adj management same use	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 22:02
S19	1	("6069957").PN.	US-PGPUB; USPAT	OR	OFF	2007/02/17 14:19
S20	1	("6772340").PN.	US-PGPUB; USPAT	OR	OFF	2007/02/17 14:19
S21	25	(key adj encrypting adj key key adj upon adj key adj encryption skeleton adj key) and graph	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 01:22
S22	504	((726/28) or (726/29)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/17 16:07
S23	267	(380/281).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/17 16:52
S25	680	(713/170).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/17 16:52

## EAST Search History

S26	95	S25 and (@pd > "20060617")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/17 16:53
S27	171	skeleton adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 21:40
S28	1	("6069957").PN.	US-PGPUB; USPAT	OR	OFF	2007/06/29 21:53
S29	887	((380/284) or (713/170)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/06/29 21:54
S30	73	S29 and (@pd > "20070217")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 00:03
S31	948	((380/284) or (713/170)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/11/18 00:03
S32	58	S31 and (@pd > "20070709")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 00:13
S33	0	(directed adj graph) same (encrypt\$3) same key same association	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 00:15
S34	3	(directed adj graph) same key same association	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 00:15
S35	0	(graph) same (decrypt\$3 encrypt\$3) near2 key same association	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 00:16

## EAST Search History

S36	119	(graph) same (decrypt\$3 encrypt\$3) near2 key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 00:16
S37	10	("20020144149"   "20020194484"   "5712914"   "5748736"   "5987376"   "6016505"   "6092201"   "6266420"   "6351813"   "6748530").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/11/18 01:14
S38	3	(node and graph and association and key and (encrypt\$3 decrypt\$3)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 01:23
S39	3	((encrypted near3 key) and rights adj management and permission and license).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/18 01:24


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide



THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

 Terms used: **skeleton key key encrypting key master key**

Found 10 of 215,186

Sort results by


[Save results to a Binder](#)
[Try an Advanced Search](#)
[Try this search in The ACM Guide](#)

Display results


[Search Tips](#)
☐ Open results in a new window

Results 1 - 10 of 10

 Relevance scale ☐ ☐ ☐ ☐ ☐

### 1 [Cryptographic key management](#)



Dahl A. Gerberick

 May 1990 **ACM SIGSAC Review**, Volume 8 Issue 2

Publisher: ACM Press

 Full text available: pdf(962.96 KB) Additional Information: [full citation](#), [abstract](#), [index terms](#)

There are two main issues concerning data security on networks; controlling access and the vulnerability of data communication links. A brief introduction to the various techniques which may be applied to these concerns are given in this paper.

### 2 [Architecture for Protecting Critical Secrets in Microprocessors](#)



Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, Zhenghong Wang

 May 2005 **ACM SIGARCH Computer Architecture News, Proceedings of the 32nd annual international symposium on Computer Architecture ISCA '05**, Volume 33 Issue 2

Publisher: IEEE Computer Society, ACM Press

 Full text available: pdf(143.62 KB) Additional Information: [full citation](#), [abstract](#), [cited by](#), [index terms](#)

We propose "secret-protected (SP)" architecture to enable secure and convenient protection of critical secrets for a given user in an on-line environment. Keys are examples of critical secrets, and key protection and management is a fundamental problem often assumed but not solved underlying the use of cryptographic protection of sensitive files, messages, data and programs. SP-processors contain a minimalist set of architectural features that can be built into a general-purpose microprocess ...

### 3 [Protecting applications with transient authentication](#)



Mark D. Corner, Brian D. Noble

 May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**

Publisher: ACM Press

 Full text available: pdf(294.40 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

#### 4 Security: Automatic discovery of API-level exploits



Vinod Ganapathy, Sanjit A. Seshia, Somesh Jha, Thomas W. Reps, Randal E. Bryant  
May 2005 **Proceedings of the 27th international conference on Software engineering  
ICSE '05 , Proceedings of the 27th international conference on Software  
engineering ICSE '05**

**Publisher:** ACM Press, IEEE Computer Society

Full text available: pdf(510.01 KB)



[Publisher Site](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We argue that finding vulnerabilities in software components is different from finding exploits against them. Exploits that compromise security often use several low-level details of the component, such as layouts of stack frames. Existing software analysis tools, while effective at identifying vulnerabilities, fail to model low-level details, and are hence unsuitable for exploit-finding. We study the issues involved in exploit-finding by considering application programming interface (API) level ...

**Keywords:** API-level exploit, bounded model checking

#### 5 Wireless network security I: Common data security network (CDSN)



Aftab Ahmad, Mona El-Kadi Rizvi, Stephan Olariu  
October 2005 **Proceedings of the 1st ACM international workshop on Quality of  
service & security in wireless and mobile networks Q2SWinet '05**

**Publisher:** ACM Press

Full text available: pdf(287.12 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We present the idea of using a separate network that processes and enforces security in a data network. We briefly discuss various components of such a network, called common data security network (CDSN). We use the example of the IEEE 802.11i to determine one of the link level metrics of the proposed network, the fractional overhead for IEEE 802.1X and temporal key integrity protocol (TKIP).

**Keywords:** IEEE 802.11i, TKIP, common data security, security architecture, security plane, wireless LANs

#### 6 Formal analysis of crypto protocols: A modular correctness proof of IEEE 802.11i and TLS



Changhua He, Mukund Sundararajan, Anupam Datta, Ante Derek, John C. Mitchell  
November 2005 **Proceedings of the 12th ACM conference on Computer and  
communications security CCS '05**

**Publisher:** ACM Press

Full text available: pdf(257.74 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The IEEE 802.11i wireless networking protocol provides mutual authentication between a network access point and user devices prior to user connectivity. The protocol consists of several parts, including an 802.1X authentication phase using TLS over EAP, the 4-Way Handshake to establish a fresh session key, and an optional Group Key Handshake for group communications. Motivated by previous vulnerabilities in related wireless protocols and changes in 802.11i to provide better security, we carry ou ...

**Keywords:** IEEE 802.11i, TLS, protocol composition logic

#### 7 Security: Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks





Mohamed Kassab, Abdelfettah Belghith, Jean-Marie Bonnin, Sahbi Sassi  
October 2005 **Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling WMuNeP '05**

**Publisher:** ACM Press

Full text available: pdf(398.42 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Recently, user mobility in wireless data networks is increasing because of the popularity of portable devices and the desire for voice and multimedia applications. These applications, however, require fast handoffs among base stations to maintain the quality of the connections. Re-authentication during handoff procedures causes a long handoff latency which affects the flow and service quality especially for multimedia applications. Therefore minimizing re-authentication latency is crucial in ord ...

**Keywords:** IAPP, IEEE 802.11i, WiFi, handover, pre-authentication, re-authentication

8 Security analysis: Analysis of the 802.11i 4-way handshake ☐



Changhua He, John C. Mitchell  
October 2004 **Proceedings of the 3rd ACM workshop on Wireless security WiSe '04**

**Publisher:** ACM Press

Full text available: pdf(328.36 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

802.11i is an IEEE standard designed to provide enhanced MAC security in wireless networks. The authentication process involves three entities: the supplicant (wireless device), the authenticator (access point), and the authentication server (e.g., a backend RADIUS server). A 4-Way Handshake must be executed between the supplicant and the authenticator to derive a fresh pairwise key and/or group key for subsequent data transmissions. We analyze the 4-Way Handshake protocol using a finite-state ve ...

**Keywords:** 4-way handshake, 802.11i, WLAN, authentication, denial-of-service, key management

9 A survey of key management for secure group communication ☐



Sandro Rafaeli, David Hutchison  
September 2003 **ACM Computing Surveys (CSUR)**, Volume 35 Issue 3

**Publisher:** ACM Press

Full text available: pdf(346.27 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Group communication can benefit from IP multicast to achieve scalable exchange of messages. However, there is a challenge of effectively controlling access to the transmitted data. IP multicast by itself does not provide any mechanisms for preventing nongroup members to have access to the group communication. Although encryption can be used to protect messages exchanged among group members, distributing the cryptographic keys becomes an issue. Researchers have proposed several different approach ...

**Keywords:** Group Key Distribution, Multicast Security

10 Lightweight key management for IEEE 802.11 wireless LANs with key refresh and host revocation ☐

Avishai Wool  
November 2005 **Wireless Networks**, Volume 11 Issue 6

**Publisher:** Kluwer Academic Publishers

Full text available:  pdf(466.01 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The IEEE 802.11 Wireless LAN standard has been designed with very limited key management capabilities, using up to 4 static, long term, keys, shared by all the stations on the LAN. This design makes it quite difficult to fully revoke access from previously-authorized hosts. A host is fully revoked when it can no longer eavesdrop and decrypt traffic generated by other hosts on the wireless LAN. This paper proposes WEP\*, a lightweight solution to the host-revocation problem. The key mana ...

**Keywords:** authentication, security

Results 1 - 10 of 10

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)